CLAIMS

What is claimed is:

1. A method comprising:

receiving a CRUable dual mode wireless card having both an ISM radio and a U-NII radio in an interface within a wireless ready device designed for receiving a radio card, said U-NII radio having a radio identification (ID) parameter, wherein said interface enables said U-NII radio to be coupled to and send signals to an antenna that is embedded in the device and which has an antenna identification (ID) parameter;

prior to enabling use of said U-NII radio and said antenna to complete a U-NII transmission, completing an authentication process that verifies that said U-NII radio is an authorized radio for utilization with the antenna and within the device under U-NII standards; and

when said authentication process verifies that a pairing of said radio and said antenna is authorized, switching a transmission mode of said device from ISM mode to U-NII mode, which enables U-NII communication via said pairing of said antenna and said radio, wherein a U-NII transmitter meeting an FCC "integral" requirement is provided within the wireless-ready device having the embedded antenna.

2. The method of Claim 1, wherein:

said CRUable dual mode wireless card also comprises storage means for holding the radio ID and interface connection pins for connecting said card to said interface of said device, wherein said interface connection pins include a fist pin for connecting each of said radios to the antenna and a second pin for connecting said card to a basic input/output system (BIOS) of the device; and

said step for completing an authentication process completes a radio-to-antenna and a radio-to-device authentication process, wherein only an authorized radio model is enabled within the device .

3. The method of Claim 2, further comprising:

activating the ISM radio at power-on to provide default wireless transmission via ISM mode;

responsive to any request for transmission that does not specify U-NII mode, completing the transmission via ISM mode; and

automatically disabling the ISM radio whenever a request for U-NII mode transmission is received and the authentication process indicates the pairing of the U-NII radio and the antenna is authorized within the device, wherein only exclusive operation in ISM mode or U-NII mode is permitted within said device.

4. The method of Claim 2, further comprising:

allowing a boot process being executed on the device to complete, wherein when said radio ID and the radio ID from the table does not match, said radio is disabled from operating within said device and said device is booted without U-NII transmission capability.

5. The method of Claim 2, wherein said enabling step further comprises:

storing an indication of said match of radio IDs within an approval flag;

checking said approval flag for said indication prior to completing a U-NII connection from said device, wherein a request for U-NII connection is allowed to proceed only when said approval flag indicates that U-NII connection is authorized and other built-in checks are satisfied; and

clearing said approval flag whenever a triggering condition is registered on the device, said triggering condition being a condition form among rebooting the device, removing the wireless module, breaking a connection between said antenna and said radio, modification/replacement of said radio, modification/replacement of said antenna.

6. The method of Claim 1, wherein said radio ID and said antenna ID are peripheral component interconnect (PCI) identifications (IDs).

7. The method of Claim 1, said authentication process further comprising:

following a power on of said device, initiating a BIOS check of system components, wherein the radio ID is read from the U-NII radio that is also electrically coupled to said BIOS;

populating a table with authorized antenna-radio ID pairs for that device;

retrieving the antenna ID from a storage location within said BIOS;

locating the antenna ID in the table of approved radio-antenna pairs;

reading an associated tabled radio ID from the approved radio-antenna pairs with the antenna ID of the embedded antenna;

comparing said radio ID of the U-NII radio against the tabled radio ID for a match of radio IDs.

8. The method of Claim 1, further comprising:

following a determination that the radio ID of the U-NII radio matches one associated with the antenna ID, providing a secret key to a device driver to trigger the device driver to activate a switch of transmission modes from ISM to U-NII mode, wherein said device driver operates as a gatekeeper to allow only authorized radios to operate within the device, and wherein said U-NII mode is deactivated until a software key authenticates the card when the comparing step results in a match.

9. The method of Claim 2, wherein further:

said device comprises the antenna, the interface, which includes a BIOS interface and an antenna interface, a coax coupling the antenna interface to said antenna, a Client Manager utility, and the BIOS, which includes a table of approved radio-antenna pairings for the device.

10. The method of Claim 9, wherein said reading and comparing steps are completed by the client manager utility, which provides a software key required to enable dynamic switching from ISM to U-NII transmission modes, said method further comprising:

providing a table of authorized pairings of radio ID and antenna IDs within a client manager utility;

initiating the comparing step; and

signaling a device driver of the device when to enable an interface, which interface is required to provide wireless transmission in U-NII mode.

11. The method of Claim 2, wherein further:

said device comprises the antenna, the interface, which includes a BIOS interface and an antenna interface, a coax coupling the antenna interface to said antenna, the BIOS, a device driver, a Validation Utility and a Windows register, which respectively provide a table of approved U-NII radio-antenna pairings and a table of approved wireless card IDs for the specific device.

12. The method of Claim 11, wherein said reading and comparing steps are completed by the validation utility, said method further comprising:

providing a table of authorized pairings of radio ID and antenna IDs within the validation utility;

populating the windows registry with a list of approved cards for that device; and

following a determination that the radio ID of the U-NII radio matches one within the table, generate a secret key that is sent to the device driver to trigger the device driver to activate a switch of transmission modes from ISM to U-NII mode, wherein said device driver operates as a gatekeeper to allow only authorized radios to operate within the device.

13. The method of Claim 11, further comprising signaling the device driver of the device when to enable an interface, which interface is required to provide wireless transmission in U-NII mode, wherein correct software key is required to enable the device driver to dynamically switch from ISM to U-NII transmission modes.

14. The method of Claim 11, said authentication process further comprising:

retrieving a secret key from a device driver, said secret key being an allowable card ID for that device;

comparing said secret key against the card's ID; and

enabling said radio to operate within said device only when said secret key matches the

card ID, wherein U-NII transmission via the radio-antenna combination is enabled only when said radio-antenna ID pairing matches one of said approved radio/antenna ID pairs within the table and said secret key matches the ID of the connected radio card.

15. The method of Claim 15, wherein said secret key is a model number of approved cards for operation within the device and said model number is associated with the radio PCI ID within the table.

16. The method of Claim 11, wherein said device is a wireless-ready computer system and said method enables heterogeneous roaming from one transmission mode to another from the wireless ready computer system utilizing approved transmitters.

17. A wireless-ready device comprising:

an embedded antenna having an antenna ID and specific design characteristics to enable ISM transmission when coupled to an ISM radio and U-NII transmission when coupled to an authorized U-NII radio;

an interface which receives a CRUable dual mode wireless card with an ISM radio and a U-NII radio having a radio ID, wherein said interface enables said U-NII radio to be coupled to and interface with the embedded antenna;

a BIOS that is linked to both the antenna and the U-NII radio and is able to acquire the radio ID and the antenna ID;

an authentication mechanism associated with said BIOS that initiates a radio-to-device verification process following a boot of the device, wherein said authentication mechanism verifies that said radio is an authorized radio for utilization with the embedded antenna and that said radio card is authorized to operated within said device according to pre-established U-NII standards; and

a device driver having U-NII transmitter activation logic that, when said verification process verifies that said radio is authorized for utilization with said antenna and said card is authorized for utilization within said device, enables U-NII transmission mode utilizing the antenna and U-NII radio combination, wherein a U-NII transmitter meeting an FCC "integral" requirement is provided within the wireless ready device.

18. The device of Claim 17, wherein:

said CRUable dual mode wireless card also comprises storage means for holding the radio ID and interface connection pins for connecting to said interface of said device, wherein said interface connection pins include a fist pin for connecting said U-NII radio to the antenna and a second pin for connecting said card to a basic input/output system (BIOS) of the device.

19. The device of Claim 18, said device driver further comprising:

logic for activating the ISM radio at power-on to provide default wireless transmission via ISM mode;

logic, responsive to any request for transmission that does not specify U-NII mode, for completing the transmission via ISM mode; and

logic for automatically disabling the ISM radio whenever a request for U-NII mode transmission is received and the authentication process indicates the pairing of the U-NII radio and the antenna is authorized within the device, wherein only exclusive operation in ISM mode or U-NII mode is permitted within said device.

20. The device of Claim 17, said authentication mechanism comprising:

activation code, which initiates a BIOS check of system components following a power on of said device, wherein the radio ID is read from the U-NII radio that is also coupled to said BIOS and the antenna ID is retrieved from a storage location for the antenna ID;

authentication code that (1) populates the table within the device with authorized antenna-radio ID pairs for that device; and (2) reads a tabled radio ID that is associated with an antenna ID within the table that is the same as the antenna ID of the embedded antenna;

a comparator that compares the radio ID with the tabled radio ID following a matching of the antenna ID with one within the table; and

a verification mechanism that, when said radio ID and said tabled radio ID matches, signals an approval of said radio-to-device authentication as a successful authentication of said radio for operation within said device.

21. The device of Claim 18, wherein:

said authentication mechanism further comprises logic that, in response to a match of the radio ID with the tabled radio ID, provides a secret key to the device driver; and

said device driver comprises logic that, when said secret key is received, compares the secret key to a card ID of the wireless card and activates a switch of transmission modes from ISM to U-NII mode only when said secret key matches the card ID, wherein said device driver operates as a gatekeeper to allow only authorized radio cards to operate within the device.

22. The device of Claim 18, wherein further:

said device driver includes logic for enabling said radio to operate within said device only when said secret key matches the card ID, wherein U-NII transmission via the radio-antenna combination is enabled only when said radio-antenna ID pairing matches one of said approved radio/antenna ID pairs within the table and said secret key matches the ID of the connected radio card.

23. The device of Claim 18, further comprising:

boot termination mechanism that allows a boot process being executed on the device to complete when said radio ID and said tabled radio ID matches, wherein when said match does not occur, said boot termination mechanism terminates said boot process.

24. The device of Claim 18, further comprising:

a transmission disabling mechanism that disables said radio from operating within said device when said radio ID and said tabled radio ID do not match or said secret key does not match the card ID, wherein said device is initially booted without U-NII transmission capability.

25. The device of Claim 18, wherein said device driver comprises a transmission disabling mechanism that disables said radio from operating within said device when said radio ID and said tabled radio ID do not match or said secret key does not match said card ID, wherein said device is booted without U-NII transmission capability.

26. The device of Claim 18, further comprising:

an approval flag that stores a result of the comparison of the radio IDs;

means for checking said approval flag for said result prior to completing a U-NII connection with said device, wherein a request for U-NII connection is allowed to proceed only when said result indicates a match between said radio IDs; and

reset mechanism for resetting a value of said validation register whenever a triggering condition is registered on the device, said triggering condition being a condition from among rebooting the device, removing the wireless module, breaking a connection between said antenna and said radio, modification/replacement of said radio, modification/replacement of said antenna.

27. The method of Claim 17, wherein further:

said authentication mechanism is a Client Manager utility; and

said device comprises the antenna, the interface, which includes a BIOS interface and an antenna interface, a coax coupling the antenna interface to said antenna, the Client Manager utility, and the BIOS, which includes a table of approved pairings of radio and antenna IDs for the device.

28. The device of Claim 18, wherein further:

said authentication mechanism includes a Validation utility and a Windows register, which respectively provide a table of approved U-NII radio-antenna pairings and a table of approved wireless card IDs for the specific device; and

said device comprises the antenna, the interface, which comprises a BIOS interface and an antenna interface, a coax coupling the antenna interface to said antenna, the BIOS, a device driver, the Validation Utility and the Windows register.

29. The device of Claim 28, said authentication process further comprising:

following a power on of said device, initiating a BIOS check of system components, wherein the radio ID is read from the U-NII radio that is also coupled to said BIOS;

populating the table within the validation utility with the authorized pairings of antenna and radio IDs for that device;

retrieving the antenna ID from a storage location within said BIOS;

reading a first radio ID from the table within the BIOS, wherein said radio PCI ID read is one stored as a paired entry in said table with the retrieved antenna ID of the embedded antenna;

comparing a pairing of said radio ID and said antenna ID against the table of approved radio/antenna ID pairs, wherein the radio IDs are compared once the retrieved antenna ID is located within the table.

30. The device of Claim 29, wherein said reading and comparing steps are completed by the validation utility, which provides the device driver with a software key required to enable dynamic switching from ISM to U-NII transmission modes, said method further comprising:

providing a table of authorized pairings of radio ID and antenna IDs within the validation utility;

initiating the comparing step; and

signaling a device driver of the device when to enable an interface, which interface is required to provide wireless transmission in U-NII mode.

31. The method of Claim 29 further comprising:

populating the windows registry with a list of approved cards for that device; and

following a determination that the radio ID of the U-NII radio matches one within the table, generate a secret key that is sent to the device driver to trigger the device driver to check the list of approved cards within the windows registry against the card ID of the wireless card, wherein said device driver activates a switch of transmission modes from ISM to U-NII mode only when said card Id matches one within the windows registry, and wherein said device driver operates as a gatekeeper to allow only authorized radio cards to operate within the device.